--11. (new) A method for transmitting signals between a transmitter and a receiver, the method comprising:

calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase; and

calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and a transmission sequence of the signals.

12. (new) The method as recited in claim 11 wherein the calculation phase includes generating a pseudo-random sequence.

13. (new) The method as recited in claim 12 wherein certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence, and wherein the authentication token of one of the signals transmitted at an i-th position is calculated as a function of the coding of the signal and the coding of the respective position in the transmission sequence.

14. (new) The method as recited in claim 13 wherein the authentication token of the one signal transmitted at the i-th position is a bit-by-bit XOR link or an equivalent logic function of the coding of the one signal and the coding of the respective position in the transmission sequence.

15. (new) The method as recited in claim 11 wherein the calculation phase includes generating a pseudo-random sequence.

16. (new) The method as recited in claim 15 wherein certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence, and wherein the authentication token of a one of the signals transmitted at an i-th position is calculated as a function of the coding of all previously transmitted signals and the coding of the respective position in the transmission sequence.

17. (new) The method as recited in claim 16 wherein the authentication token of the one signal transmitted at the i-th position is a bit-by-bit XOR link or an equivalent logic link of the coding of all the previously transmitted signals and the coding of the respective position in the transmission sequence.

18. (new) The method as recited in claim 11 wherein the at least one cryptographic algorithm includes a block cipher.

19. (new) The method as recited in claim 18 wherein the block cipher includes a data encryption standard.

20. (new) The method as recited in claim 12 wherein the at least one cryptographic algorithm includes a block cipher, the pseudo-random sequence being generated by operating the block cipher in a known output feedback mode.

21. (new) The method as recited in claim 15 wherein the at least one cryptographic algorithm includes a block cipher, the pseudo-random sequence being generated by operating the block cipher in a known output feedback mode.

22. (new) The method as recited in claim 11 wherein the communication phase further includes calculating another token for authentication of the transmitter, the other token being subsequently transmitted so as to initialize the receiver for authentication of the transmitter.

23. (new) The method as recited in claim 11 further comprising confirming the transmission sequences by nonintersecting m-bit strings.--

REMARKS

This Preliminary Amendment cancels original claims 1-10 in the underlying PCT Application No. PCT/EP97/05081, and adds new claims 11-23. The new claims do not add new matter to the application but do conform the claims to U.S. Patent and Trademark Office rules.